Los retos tecnológicos: cómo abordarlos

(desde la perspectiva de un OCEX)

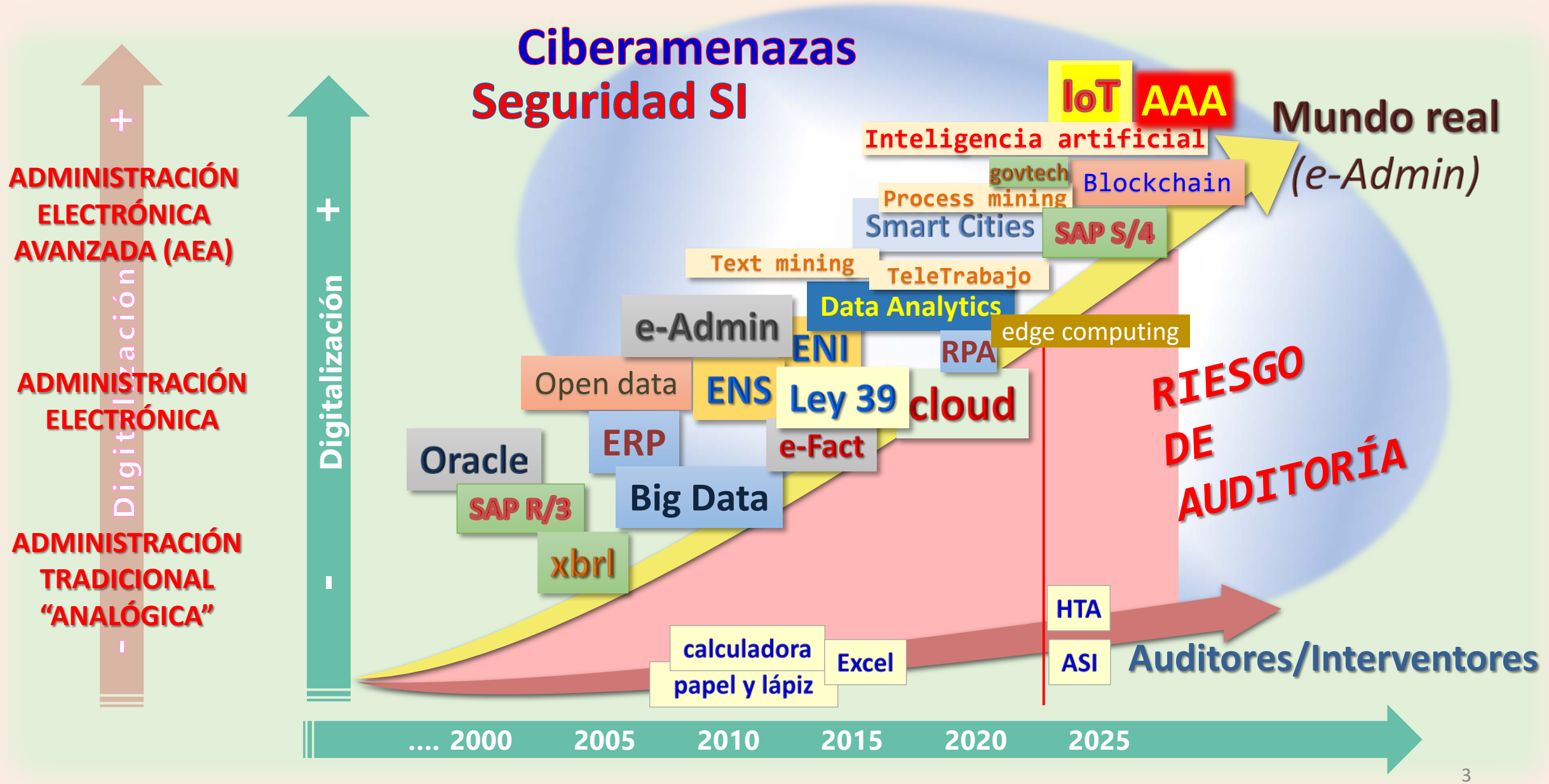
Unidad de Auditoría de Sistemas de Información

Antonio Minguillón Roy

Auditor director del gabinet tècnic de la Sindicatura de Comptes de la Comunitat Valenciana.

Entorno de trabajo del auditor público: la AEA

La complejidad de la tecnología y los riesgos de auditoría crecen …



TIC/AEA: Riesgos para el auditor/interventor

Resumiendo ....

- Pérdida de evidencia visible y de pistas de auditoría
- Volúmenes enormes de datos
- Tecnologías emergentes
- Ciberamenazas
- Riesgos TIC
- Falta de conocimientos tecnológicos
- Metodología de auditoría obsoleta
- …

TIC: Oportunidades para el auditor

Resumiendo ....

- Disponibilidad de herramientas TIC muy potentes
- Test del 100% de la población
- Conocimiento más profundo del auditado
- Mejora del análisis y valoración del riesgo
- Inteligencia artificial / asistida
- Más capacidad de análisis (datos+texto)
- ....

Principales retos que deben abordar los Auditores Públicos

- Administración electrónica AVANZADA
- Big Data+IoT
- Cloud+Edge
- Ciberseguridad
- Técnicas de análisis de datos
- Visualización de datos
- *Auditoría de sistemas de información*
- Inteligencia Artificial

Transformación *o* *Revolución Digital* del Auditor Público

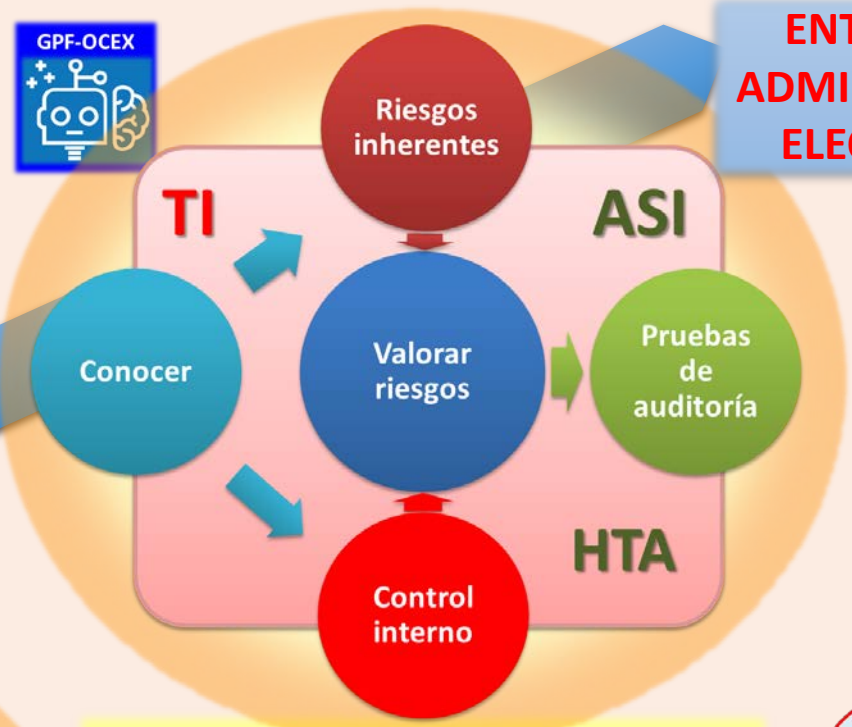
RIESGOS ineludibles

OPORTUNIDADES escurridizas

ACCIÓN necesaria

Auditoría financiera: las NIAs

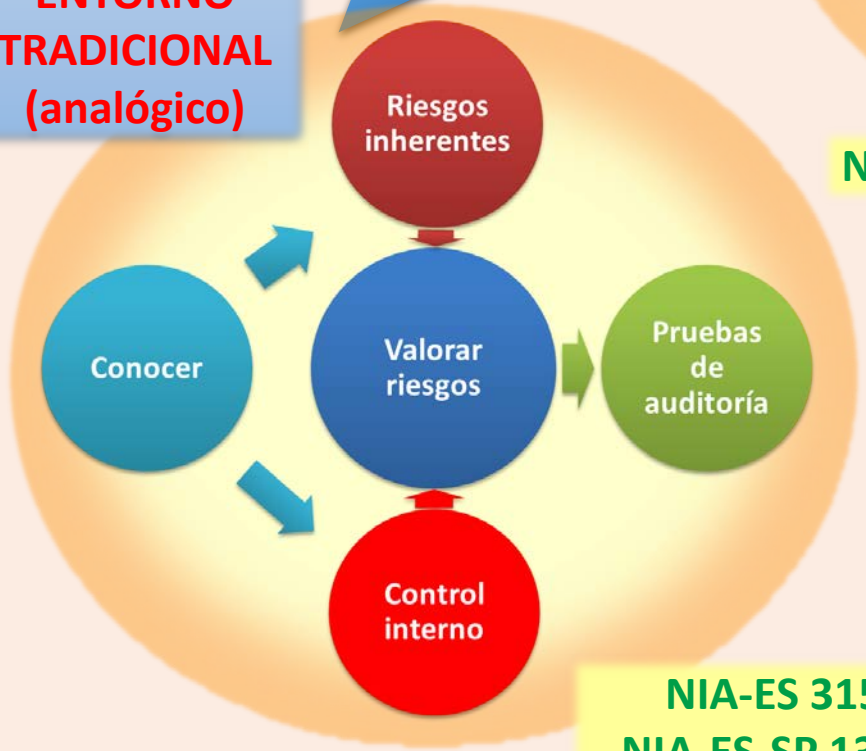
El enfoque de riesgo es el elemento central de las NIA-ES-SP



ENTORNO DE ADMINISTRACIÓN ELECTRÓNICA

NIA-ES-SP 1315 + GPF-OCEX 1315

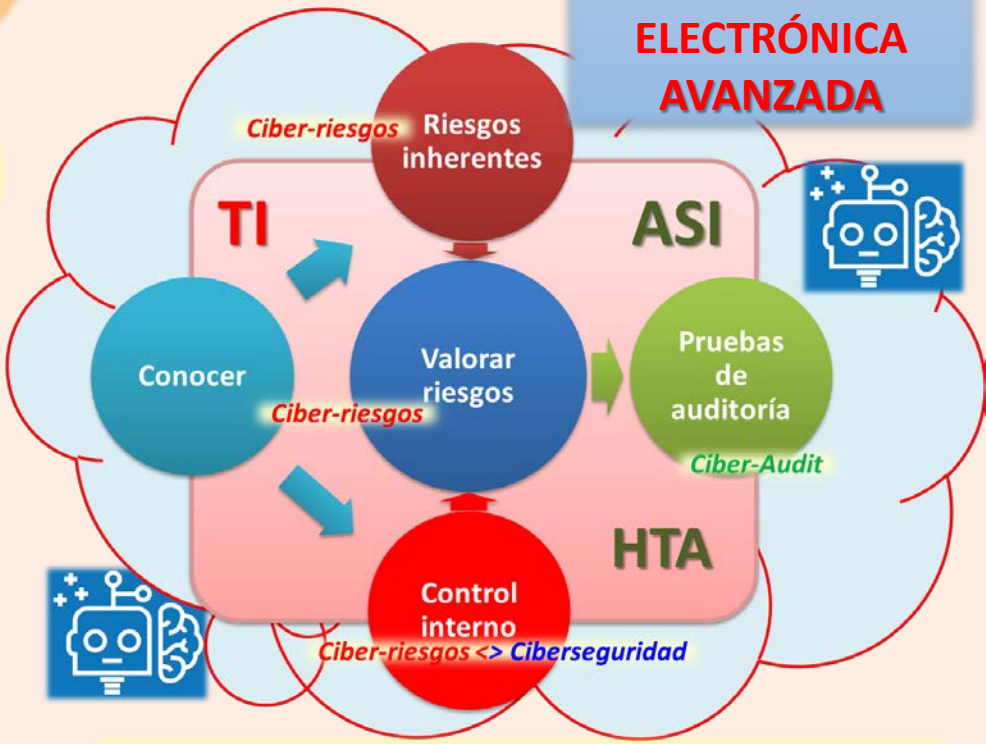
ENTORNO TRADICIONAL (analógico)



NIA-ES 315
NIA-ES-SP 1315

Adaptación

ENTORNO DE ADMINISTRACIÓN ELECTRÓNICA AVANZADA



NIA-ES 315(Revisada) + GPF-OCEX 1315R

NORMA INTERNACIONAL DE AUDITORÍA 315 (REVISADA)

IDENTIFICACIÓN Y VALORACIÓN DEL RIESGO DE INCORRECCIÓN MATERIAL

NIA-ES 315 (REVISADA)

(adaptada para su aplicación en España mediante Resolución del Instituto de Contabilidad y Auditoría de Cuentas, de 14 de octubre de 2021)

¡¡Novedad para 2023!!

Guía práctica de fiscalización de los OCEX

GPF-OCEX 1315 Identificación y valoración del riesgo de incorrección material (Revisada)

Referencia: NIA-ES 315 (Revisada)

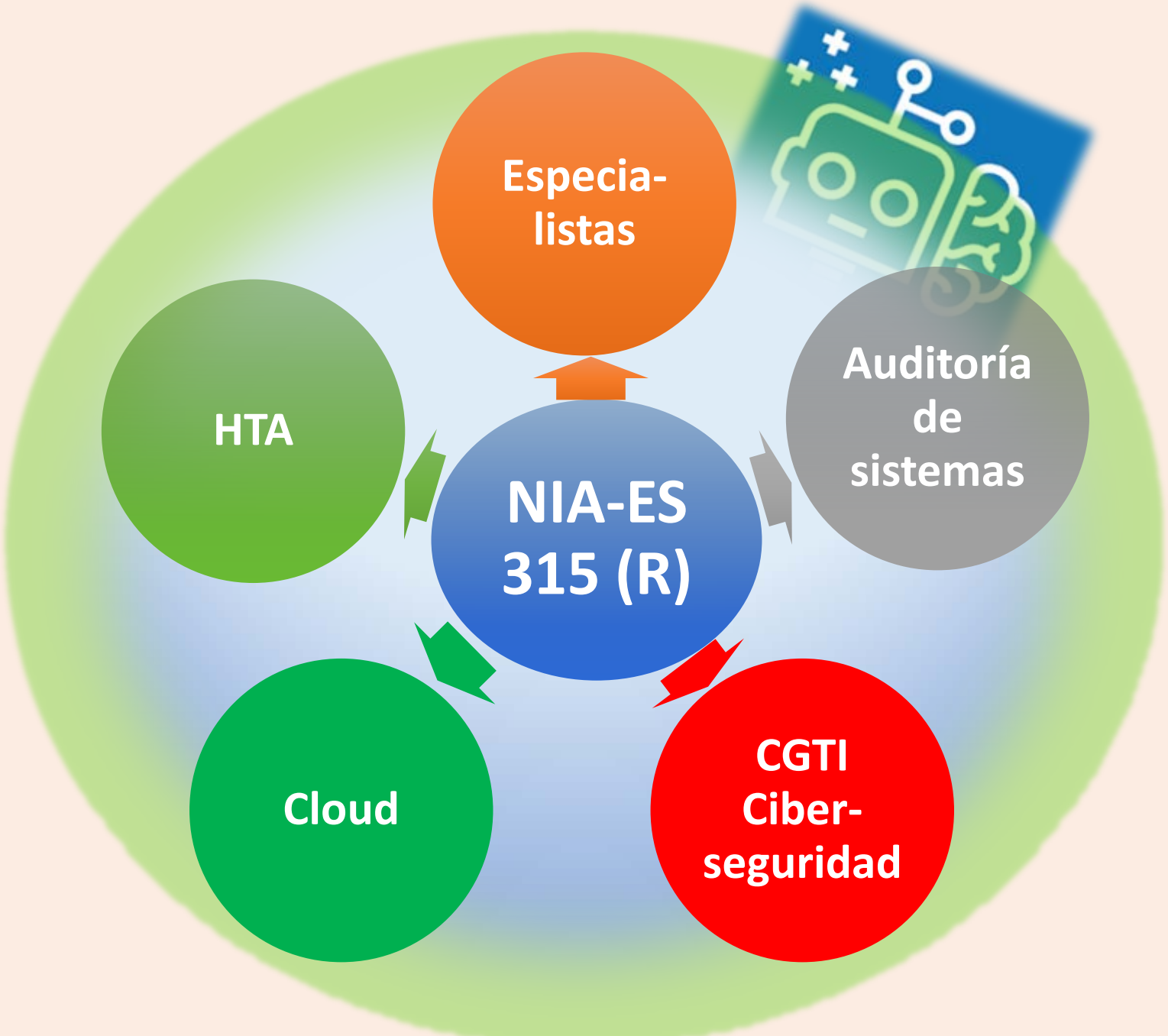
Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de la ASOCEX el 03/11/2022

Guía práctica de fiscalización de los OCEX

GPF-OCEX 1316 Guía de implementación por primera vez de la GPF-OCEX 1315 (Revisada)

Referencia: GPF-OCEX 1315 (Revisada)

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de la ASOCEX el 03/11/2022


Especia-
listas
HTA
NIA-ES
315 (R)
Auditoría
de
sistemas
Cloud
CGTI
Ciber-
seguridad

Auditoría de sistemas de información

¿Qué es la Auditoría de Sistemas de Información?

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5300 Guía de auditoría de sistemas de información

Referencia: GUID 5100 Guidance on Audit of Information Systems, aprobada en el XXIII INCOSAI, 09/2019

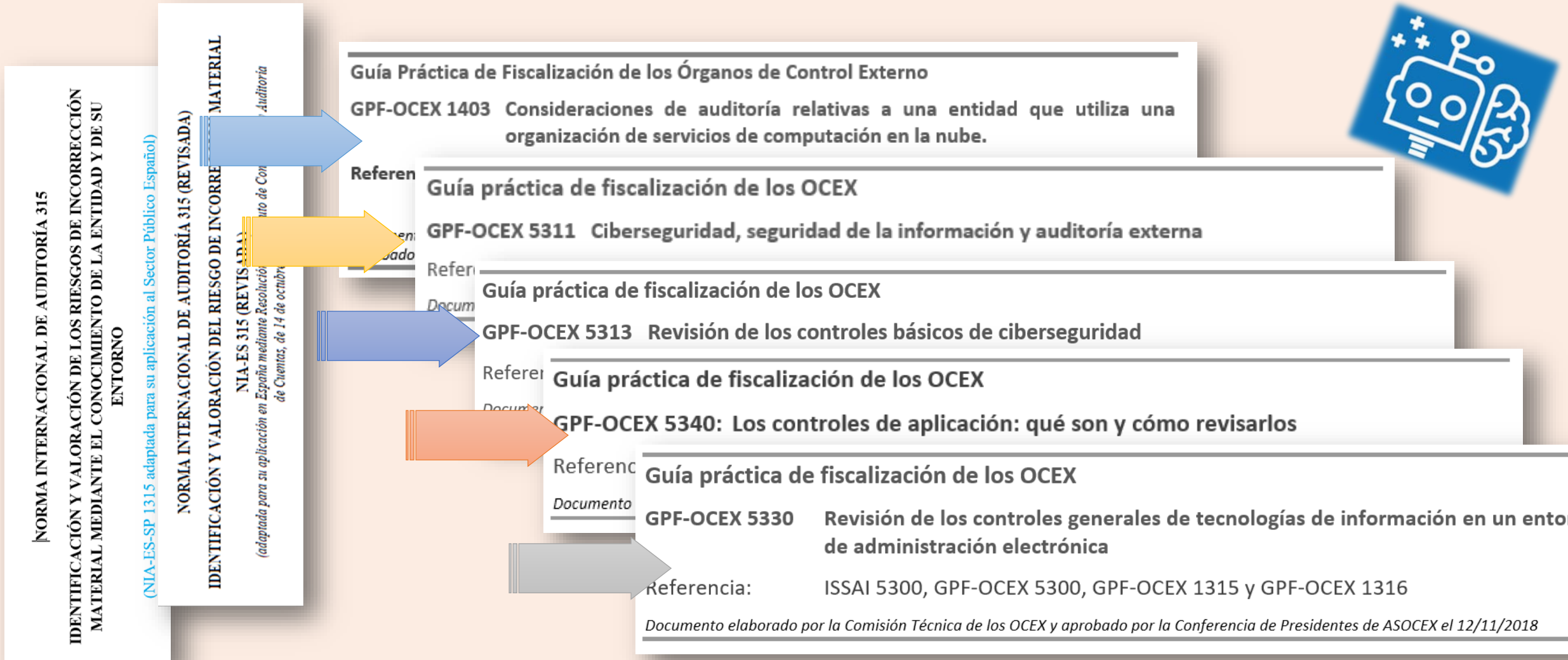
Documento elaborado por la Comisión Técnica de los OCEX el 23/10/2020
aprobado por la Conferencia de Presidentes de ASOCEX el 03/12/2020

3. Definiciones

3.1 **Sistemas de información**. Un sistema de información es un conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. Los elementos de un sistema de información son: hardware, software, soportes de información, comunicaciones, instalaciones, personal y servicios provisionados por terceros.

3.2 **Auditoría de sistemas de información**. Puede definirse como el examen de los controles relacionados con los sistemas de información y comunicaciones, a fin de identificar los casos de desviación de los criterios, que a su vez se han identificado en función del tipo de auditoría (auditoría financiera, auditoría de cumplimiento o auditoría operativa).

Guías de ASI complementarias de las NIA-ES-SP para auditar en un entorno de administración electrónica avanzada



Ciberseguridad

Los retos tecnológicos de la gestión del sector público

La ciberseguridad

El éxito de la transformación digital depende, en gran medida, de garantizar la ciberseguridad.

Por otra parte, la total dependencia de los sistemas de información y de comunicaciones existente en la gestión pública hace que las Administraciones públicas sean más vulnerables frente a los ciberataques, de modo que la transformación digital debe ir inseparablemente unida a la ciberseguridad.

¿Porqué es importante la ciberseguridad?

AMB Àrea Metropolitana de Barcelona

Català

L'àrea metropolitana AMB Territori Habitatge Ecologia Mobilitat Desenvolupament socioeconòmic

Incidència a la tramitació electrònica

Per causes externes, els sistemes de l'AMB han quedat afectats i la tramitació electrònica, altres serveis digitals i l'actualització del web no estan disponibles en aquests moments.

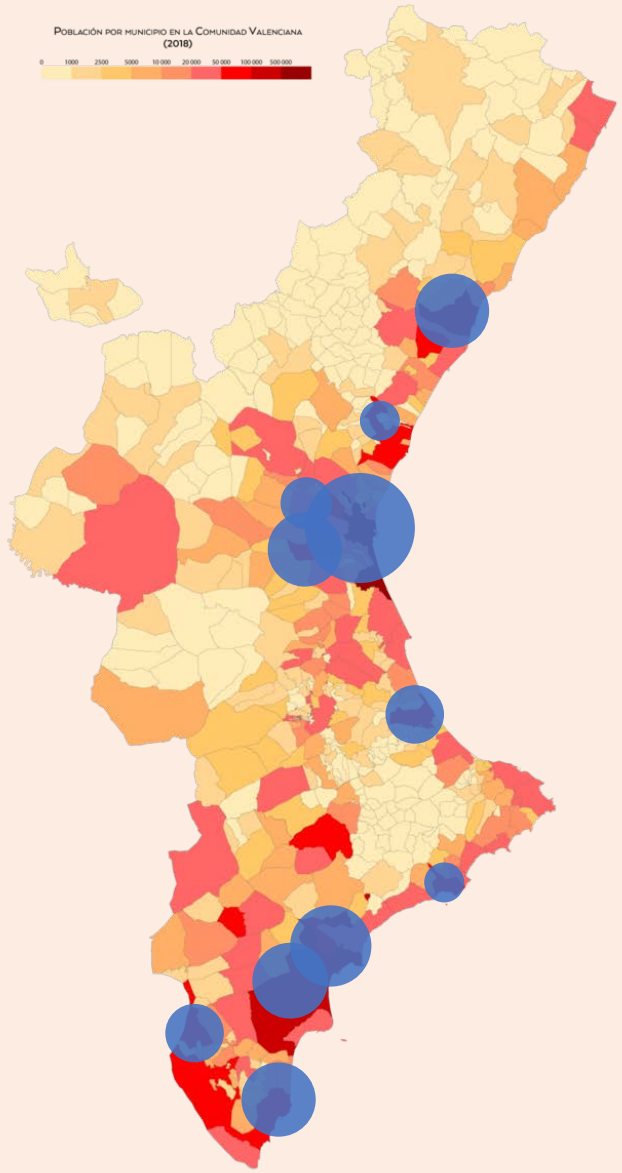
El ciberataque al Hospital Clinic de Barcelona tardará semanas en solucionarse

Los casos de ataque por ransomware son persistentes y la complejidad de los sistemas hospitalarios tampoco ayuda a una solución rápida

Resultado de las auditorías de ciberseguridad en el sector local de la CV

Ámbito subjetivo

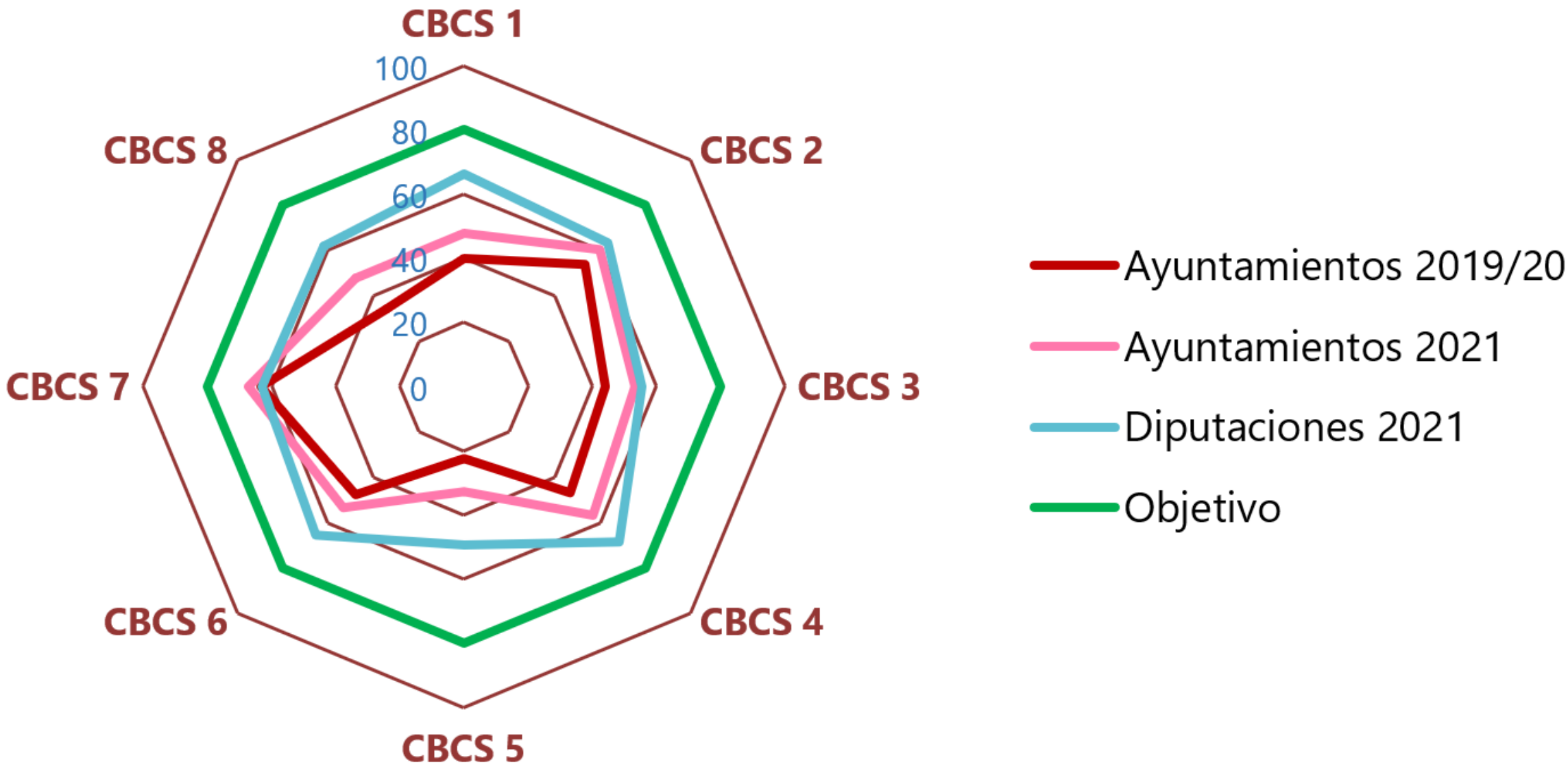
Ayuntamiento	Población 2021	ORN 2021
València	789.744	956,5
Alicante/Alacant	337.304	263,8
Elche/Elx	234.205	202,9
Castelló de la Plana	172.589	178,7
Torrent	84.025	63,0
Torrevieja	82.842	108,7
Orihuela	78.940	81,1
Gandia	75.970	95,8
Paterna	71.361	63,6
Benidorm	69.118	103,5
Sagunto/Sagunt	67.043	75,3
Alcoy/Alcoi	59.128	58,5
San Vicente del Raspeig/Sant Vicent del Raspeig	58.912	41,1
Elda	52.551	42,7
Vila-real	51.130	53,8
Ayuntamientos auditados	**2.284.862**	**2.389,0**
Población de la Comunitat Valenciana	**5.058.138**	**5.288,4**
Cobertura de la auditoría	**45,2%**	**45,2%**



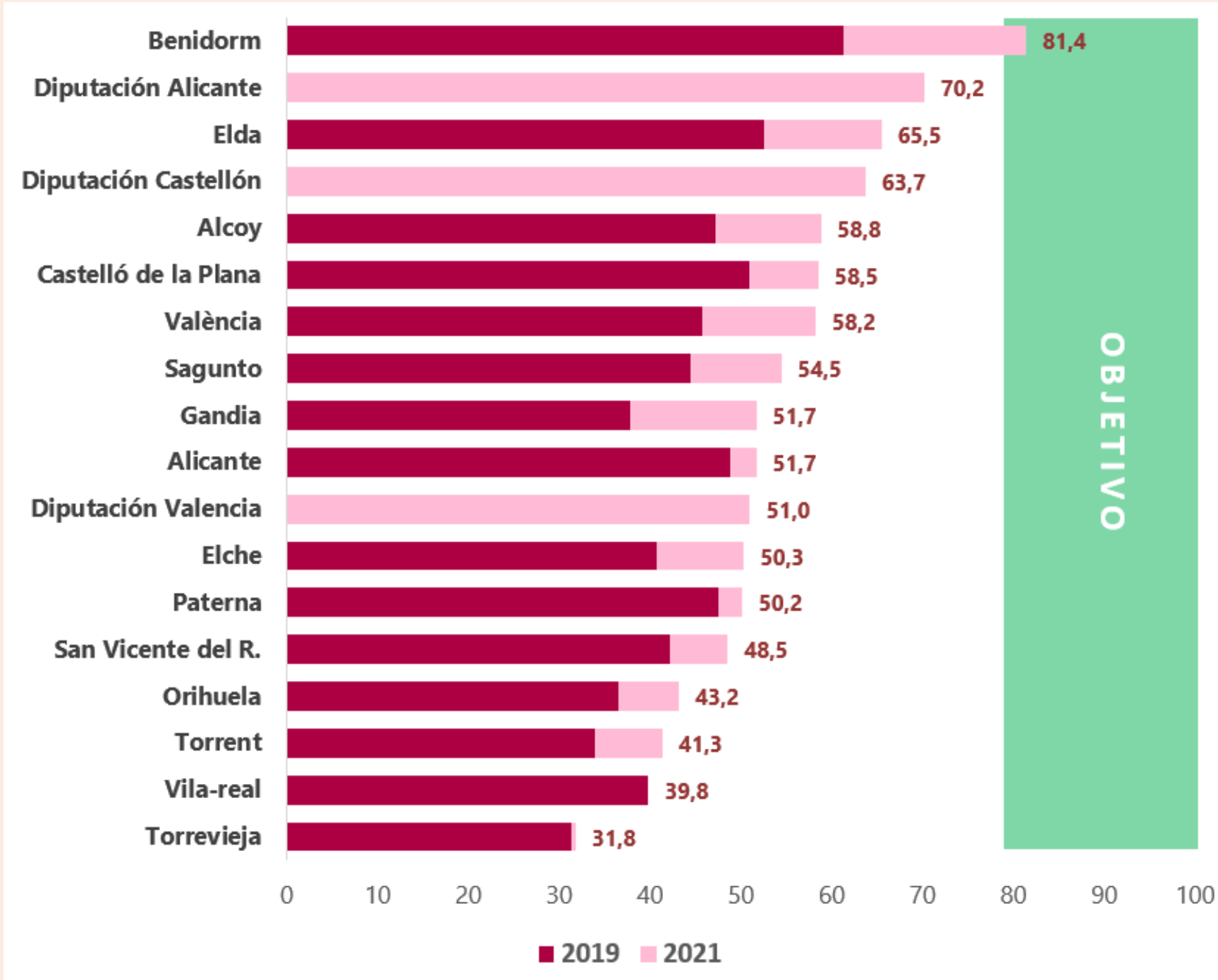
Situación de los CBCS

Control	AYUNTAMIENTOS 2019/2020 Índice de madurez	Nivel de madurez	Índice de cumplimiento	AYUNTAMIENTOS 31/12/2021 Índice de madurez	Nivel de madurez	Índice de cumplimiento	DIPUTACIONES 30/09/2021 Índice de madurez	Nivel de madurez	Índice de cumplimiento
CBCS 1 Inventario y control de dispositivos físicos	40,1%	N1	50,1%	47,7%	N1	59,6%	66,3%	N2	82,9%
CBCS 2 Inventario y control de *software* autorizado y no autorizado	53,6%	N2	67,0%	60,1%	N2	75,2%	63,3%	N2	79,2%
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	44,2%	N1	55,3%	53,2%	N2	66,5%	55,5%	N2	69,3%
CBCS 4 Uso controlado de privilegios administrativos	47,0%	N1	58,7%	56,8%	N2	71,0%	68,3%	N2	85,4%
CBCS 5 Configuraciones seguras del *software* y *hardware*	22,3%	N1	27,9%	32,6%	N1	40,7%	49,2%	N1	61,5%
CBCS 6 Registro de la actividad de los usuarios	47,7%	N1	59,6%	53,2%	N2	66,5%	65,6%	N2	82,0%
CBCS 7 Copias de seguridad de datos y sistemas	63,2%	N2	79,0%	67,3%	N2	84,1%	62,9%	N2	78,6%
CBCS 8 Cumplimiento normativo y gobernanza de ciberseguridad	34,4%	N1	43,0%	48,0%	N1	60,0%	61,7%	N2	77,1%
General	44,1%	N1	55,1%	52,4%	N2	65,4%	61,6%	N2	77,0%

Índice de Madurez MEDIO de los CBCS de los 15 mayores EELL de la CV



Índice de Madurez de los CBCS de los 18 mayores EELL de la CV



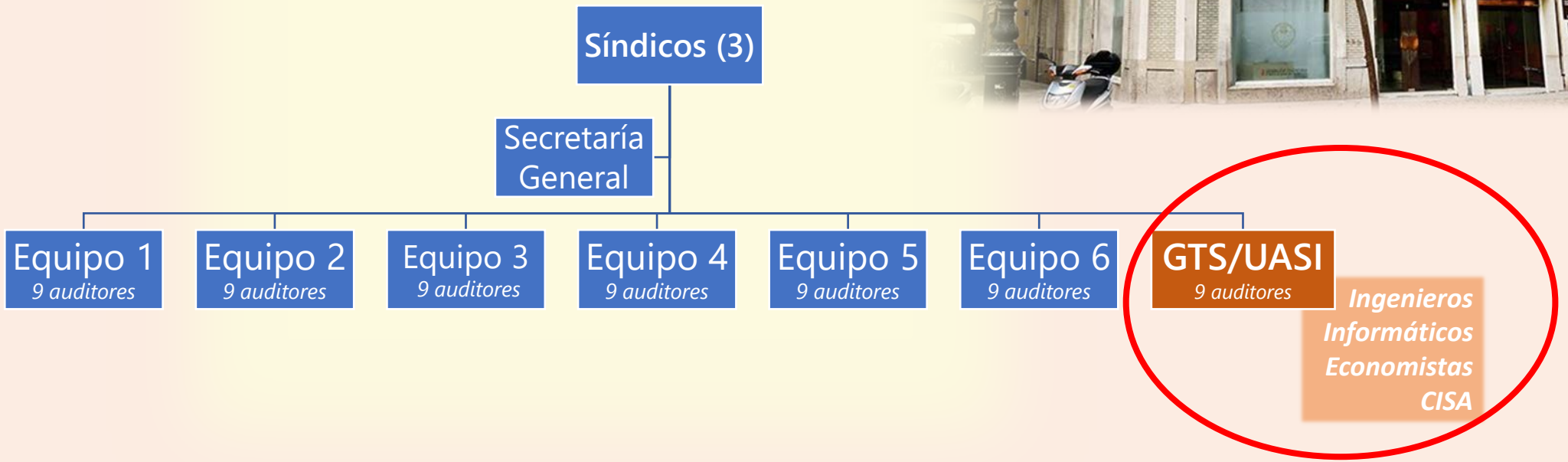
La SCCV

y

la UASI

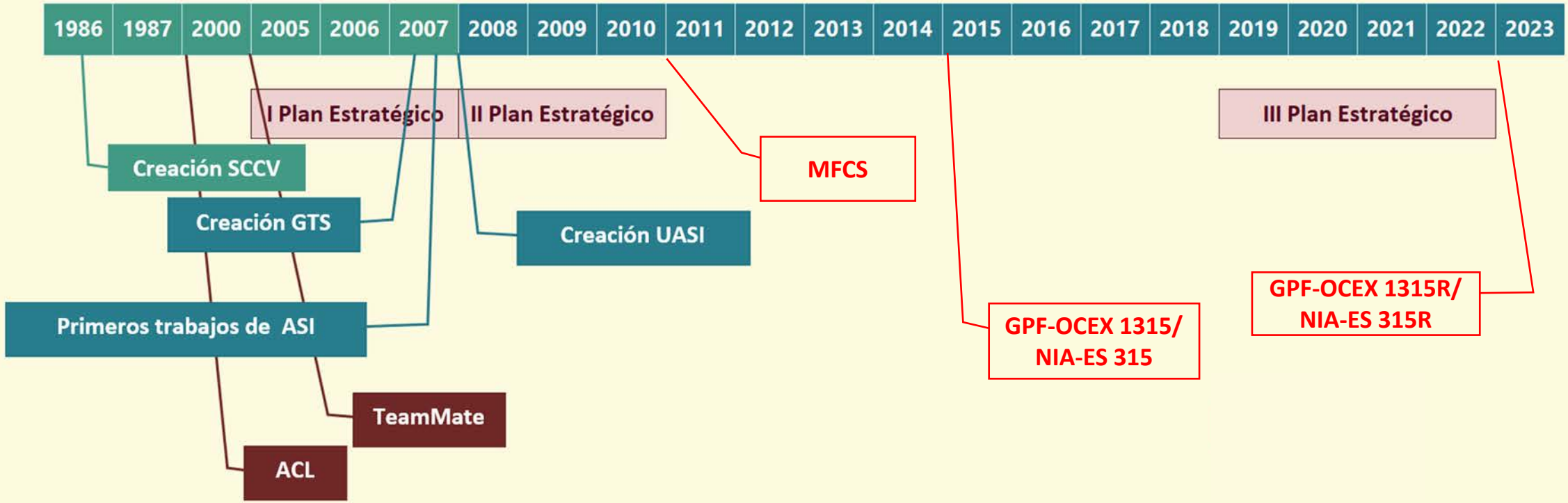
Sindicatura de Comptes de la Comunitat Valenciana

Creada en 1986
actualmente tiene 100 empleados



Evolución de la UASI

		0%	0%	0%	0%	0%	4%	6%	6%	7%	7%	7%	7%	7%	7%	11%	11%	11%	11%	11%	14%
GTS/UASI	-	-	-	-	-	-	2	3	3	4	4	4	4	4	4	7	7	7	7	7	9
Resto auditores		20	41	47	48	48	50	50	50	50	50	50	50	50	50	54	54	54	54	54	54
TI		1	2	4	4	4	4	4	4	4	4	4	4	4	4	6	6	6	6	8	10
Resto personal		10	27	33	33	33	33	33	33	33	33	33	33	33	33	29	29	29	29	27	27
Síndicos (3)		6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
TOTAL		37	76	90	91	91	95	96	96	97	97	97	97	97	97	102	102	102	102	102	106



Qué hace la UASI

- **Asistencia en las auditorías financieras, de cumplimiento y operativas (50%):**
  - ✓ Revisión de procesos automatizados, evaluación de riesgos TI, identificación y pruebas de CGTI y CPI.
  - ✓ Pruebas masivas de datos.

- **Realizamos nuestras propias auditorías:**
  - ✓ Ciberseguridad *(>35 informes)*.
  - ✓ Auditorías de control interno, CGTI y CPI *(>30 informes)*.
  - ✓ Gestión de grandes proyectos TI *(3 informes)*.

- **Promover el desarrollo de metodología de auditoría en entornos de Administración Electrónica Avanzada:**
  - ✓ Comisión Técnica de Auditoría de la Sindicatura
  - ✓ Comisión Técnica OCEX

Principales proyectos y prioridades de la UASI

- **Finalizar auditorías en marcha:**
  - ✓ Auditoría en SAP S/4 HANA: actualizar programas (CGTI+CPI) y scripts HTA
  - ✓ Auditoría de la gestión del proyecto de implantación de SAP S/4 HANA, en la Generalitat
  - ✓ Auditoría control interno del servicio sanitario, incluyendo piloto y desarrollo de metodología de Minería de procesos
- **Actualizar metodología (en marcha):**
  - ✓ En general, adoptar la nueva NIA-ES 315R / GPF-OCEX 1315R
  - ✓ En ciberseguridad, adaptar guías al nuevo ENS y CIS v8
  - ✓ HTA: mejorar el acceso directo a las bases de datos de los auditados
- **Prioridades futuras (2024)**
  - ✓ IoT, Auditoría de algoritmos, Minería de textos, IA/ML

Gracias por su atención